Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application.

Listing of Claims:

1. **(Currently Amended)** Method of establishing a trustworthiness level (TL) of a participant (2) in a communication connection between a first communication partner (1) and a second communication partner (3) and for adapting communication behaviour to the established trustworthiness level (TL), whereby said participant (2) is equipped with a trustworthiness certificate (6) and a therefrom separated securely stored participant private key (8) and that said first communication partner (1) receives said trustworthiness certificate (6) from said participant (2), wherefrom said trustworthiness level (TL) is derived and established and said first communication partner (1) tests whether said trustworthiness certificate (6) belongs to said participant (2) using said participant private key (8) and that in case said trustworthiness certificate (6) is confirmed by said test to belong to said participant (2), said first communication partner (1) communicates said established trustworthiness level (TL) to said second communication partner (3) and that at least one parameter of said communication behaviour is chosen in dependence of said established trustworthiness level (TL) , characterized in that the first communication partner (1) communicates the established trustworthiness level (TL) to the second communication partner (2) by piggybacking a trustworthiness level information (TLT)

onto a communication message, signing said communication message with a first-partner private key (13) and sending it to said second communication partner (3).

2. **(Original)** Method according to claim 1, characterized in that the trustworthiness certificate (6) arrives at the first communication partner (1) signed with a signature (9), produced with a certificate authority private key, and that said first communication partner (1) authenticates said signature (9) using a certificate authority public key (17).

3. **(Original)** Method according to claim 2, characterized in that the certificate authority public key (17) is read from a storage of the first communication partner (1).

4. **(Cancelled)**

5. **(Currently Amended)** Method according to claim 43, characterized in that the authenticity of the trustworthiness level information (TLT) Of the communication message is testable by the second communication partner (3) by using a first-partner public key (I I)-

6. **(Original)** Method according to one of claims 1 to 5, characterized in that as one of the parameters of the communication behaviour which is chosen in dependence of the established trustworthiness level (TL), is chosen the amount or number of a valuable asset, e.g. a maximum number of financial transactions and/or a maximum financial value of a financial transaction and/or a maximum number of confidential words.

7. (**Original**) Method according to one of claims 1 to 6, characterized in that the test whether the trustworthiness certificate (6) belongs to the participant (2) is performed in that a test number (R_t) is transmitted by the first communication partner (1) to said participant (2) from where said test number (R_t) returns signed under use of the participant private key (8) and in that the signature of the returning test number (R_t) is verified by using a participant public key (7) which corresponds to said participant private key (8).

8. (**Original**) Method according to claim 7, characterized in that the participant public key (7) is received by the first communication partner (1) as content of the trustworthiness certificate (6).

9. (**Original**) Method according to claim 7 or 8, characterized in that the trustworthiness level (TL) is established in that for each trustworthiness level (TL) a different trustworthiness certificate (6) with a corresponding pair of participant public key (7) and participant private key (8) is used.

10. (**Currently Amended**) Method of establishing the trustworthiness. level (TL) of a participant .(2) in a communication connection between a first communication partner (1) and a second communication partner (3) and for adapting communication behaviour to the established trustworthiness level (TL), whereby said participant (2) is equipped with a securely stored participant private key (8) and that said first communication partner (1) performs an authentication test using said participant private key (8) which also leads to establishing said trustworthiness level (TL) and that in case of

a successful authentication said first communication partner (1) communicates the established trustworthiness level (TL) to said second communication partner (3) and that at least one parameter of said communication behaviour is chosen in dependence of said established trustworthiness level (TL), characterized in that the authentication test is performed in that a test number (R_t) is transmitted by the first communication partner (1) to the participant (2) from where said test number (R_t) returns signed under use of the participant private key (8) and in that the signature of the returning test number (R_t) is verified by using a participant public key (7) which corresponds to said participant private key (8).

11. **(Canceled)**